**intel** ®

# The Wireless City

## Enhancing Productivity, Efficiency and Lifestyle

As wireless networking becomes a mainstream reality for businesses and consumers, forward-thinking cities are moving to deploy high-bandwidth, citywide networks to support government workers, local businesses and residents. With careful planning and phased deployments, wireless solutions can deliver positive returns on investment (ROI) in short order. They can also pave the way for ubiquitous connectivity that will revolutionize the way people live, work and play.

December 2003

# Table of Contents

# Executive Summary

Many local and regional governments are facing budget shortfalls in the wake of the recent economic downturn. This presents city and county planners with some tough choices: increase revenue through higher taxes; find ways to do more with less; or cut services to constituents. Certainly there is no simple solution to this challenge, yet wireless mobile technology can play a critical role by increasing worker efficiency and reducing total costs for service delivery. Moreover, a phased implementation can deliver quick payback, providing short-term gains while laying a foundation for long-term growth.

Some of the most important and direct benefits of wireless technology are derived from productivity gains. Mobile professionals with wireless notebooks can be up to 35% more productive than their counterparts with desktop PCs.[1] Benefits are especially pronounced for field workers, such as building, facility and health inspectors, social workers, emergency teams and event coordinators. Well-equipped mobile workers carry their offices with them wherever they go. They can instantly access and share schedules, forms, e-mail, client files and back-office data. They can coordinate with colleagues and supervisors more easily, both within and beyond their organization.

A wireless network can also be used to improve service delivery by dramatically reducing the costs of deploying interactive kiosks, cameras, microphones and other wireless-enabled devices. From security and traffic monitoring, to parking fine payments and tourist support, wireless devices in public spaces and government buildings can reduce costs while improving services for citizens and visitors.

Ultimately, the value of a wireless network goes beyond cost savings and service enhancements. A citywide infrastructure will help to attract new businesses and residents, and empower existing ones to be more productive. Cities that deploy their own networks may also be able to generate revenue through business arrangements with wireless service providers. In doing so, they will be creating an environment in which every-one in their city can work and play more safely and effectively.

---

[1] Analysts from Gartner Inc. have estimated the productivity gains for professionals with wireless notebooks at approximately 14 hrs/week, in comparison with the same individuals equipped with standard, wired desktops. *Desktop PCs: Technology Overview*, Gartner Dataquest, Inc., August 2002.

Culture and technology are ripe for citywide wireless solutions. IDC estimates there will be 100,000 public hotspots globally by 2005. This is in addition to the millions of private wireless networks deployed by consumers and businesses. The ratification of the IEEE 802.16a Wireless MAN standard in January of 2003 has opened the door to standards-based products that will support affordable wireless networks on a metropolitan scale. These products will complement existing 802.11 WLAN technologies, enabling high-bandwidth wireless solutions that are flexible, cost-effective and manageable.

Forward-thinking city governments are already working to deploy wireless infrastructures. This paper provides information and recommendations for validating wireless benefits in your own city, and for planning a cost-effective, scalable and secure implementation. It also describes two noteworthy examples of wireless cities in the making: The City of Westminster in England; and Rio Rancho, New Mexico in the United States.

# Empowering Government Workers

### Wireless in the Office

> *"Through 2005, more than 65 percent of the Fortune 2000 companies will adopt mobile applications."*
> —Gartner Dataquest

Businesses have good reasons for adopting wireless applications. Analysts at Gartner have estimated productivity gains at 14 hours per week for professionals with wireless notebooks.[2] Mobile workers have consistent access to business information and collaborative tools, whether they are at their desk, in a conference room, visiting a client or using a public hotspot at an airport or café. When the majority of the workforce is wireless-enabled, everyone becomes more accessible and responsive, and information flows more efficiently throughout an organization.

Clearly, these benefits are as valid for government organizations as they are for private corporations. Many government workers spend time away from their desks interacting with a wide variety of individuals, and expend considerable effort documenting their activities and communications. Mobile access to optimized office tools and applications can help automate and streamline time-consuming transactions and processes, and may add many hours of productive time to a typical work week.

### Wireless in the Field

The benefits of wireless mobility are even greater for workers who spend most of their time outside the office. Governments have a profound need for the efficiencies of wireless networking for emergency and security personnel, social service workers, inspectors, public educators and event coordinators. These and other well-paid professionals may spend many hours a day in unnecessary trips to and from the office, and in transcribing handwritten notes to document their activities and update databases. They may also lose considerable time revisiting clients and issues because they lacked key information during on-site visits. These kinds of field inefficiencies drain budgets and can take a heavy toll on service quality. In many cases, they also delay information updates to centralized applications, causing organizations to be inherently slower to respond to new developments.

Gartner reports a minimum of $34,560 annual savings per worker for users with notebooks who spend 20 percent or more of their time out of the office.[3] Mobile workers can access real-time information using consistent tools and applications as they move between the office and the field; they spend less time synchronizing applications, data and paperwork; and they can collaborate on the go with colleagues in both their own and other organizations. For workers who spend much of their time in the field, shared office space may be appropriate, providing another opportunity for substantial cost savings.

Wireless networking also reduces the cost of installing cameras, microphones, information kiosks and other wireless devices. These devices can be installed virtually anywhere, without tearing up streets or sidewalks to run network cables. Centralized security monitoring becomes an effective option for supplementing field personnel, thus reducing operational costs. A wireless network can also be used to support real-time monitoring of traffic, weather and public utilities. Problems or abnormalities can be detected instantly, and essential data can be collected in real time to improve control and planning.

---

[2] Ibid Gartner Dataquest.
[3] Ibid.

# Empowering Citizens

## Automating Key Services

Banks, grocery stores and libraries around the world are reducing wait times and service costs by deploying automated tellers and checkout machines. Interactive kiosks offer similar benefits for government agencies, especially when the kiosks can be installed and managed virtually anywhere, indoors or out, with the aid of wireless communications. Common time-consuming tasks can be automated, such as the submission of license applications and renewals, payment of parking fines and payment of taxes. Kiosks can also provide information for residents and tourists, and can include the ability to book tickets or reserve accommodations.

For government agencies, this means fewer individuals can support more people. For residents and visitors, it means shorter lines and faster, more convenient access to information and services. Instead of driving to a centralized facility, such as a government motor vehicles office, they can access services at conveniently located kiosks.

## The Wireless Lifestyle

Technology analysts at IDC have predicted there will be 105 million mobile workers by the end of 2006. Perhaps the most compelling reason for this mass adoption is the value placed on wireless solutions by individuals. Once they try it, people rarely want to give it up. Wireless mobility can have a pervasive influence in simplifying our complex lives as we seek to integrate business demands with private responsibilities. Whether it's the daily commute, a day at home with a sick child, or a few hours waiting for a car to be serviced, mobile workers can take care of business without neglecting personal priorities—and vice versa.

According to a research[4] study by NOP World-Technology, 87 percent of wireless users believe WLAN improves their quality of life by increasing flexibility, productivity and time savings. For these individuals, a citywide wireless infrastructure would dramatically improve their ability to stay connected and productive as they live, work, play and access government services. As the number of wireless-enabled individuals continues to grow, a wireless infrastructure could become a significant differentiator among cities, attracting new businesses and new residents who value the advantages of ubiquitous connectivity.

# Critical Components of the Wireless City

End-to-end wireless networking on a citywide scale is now practical and cost-effective. Wireless standards and technology road maps have solidified sufficiently to protect investments and provide scalable solutions. The popularity of these solutions has driven down costs. Equally important for outdoor implementations, new standards have emerged to fill service gaps and enable comprehensive solutions covering extensive distances.

An end-to-end wireless solution can be based on the following standards, technologies and strategies (Figure 1):

- **IEEE 802.11 Wireless LAN (Wi-Fi)** for indoor and outdoor hotspots.

- **IEEE 802.16a Wireless MAN (WiMAX)** for connecting 802.11 access points to the Internet and government networks, bridging buildings and filling in service gaps across metropolitan-sized areas.

- **Intel Technology-based Notebooks and Handheld Devices** that are designed from the ground up for the demands of wireless mobility.

- **Mobilized Applications** that enable seamless productivity as workers move between the office and the field.

- **Controlled Access and Security** to protect the privacy and integrity of wireless communications.

Each of these components is discussed in detail below.

## IEEE 802.11—Wireless Local Area Networks

Millions of 802.11 wireless access points are currently in use, providing effective wireless connectivity both indoors and out (typically within about 100 meters of the access device). All together, they form a rapidly growing public and private infrastructure that includes corporate LANs, public hotspots and home networks. Affordable 802.11 access points, along with compatible notebook computers and handheld devices, are widely available, and can be supported today with strong and cost-effective security solutions.

---

[4] The study was prepared for Cisco Systems by NOP World-Technology (2001).
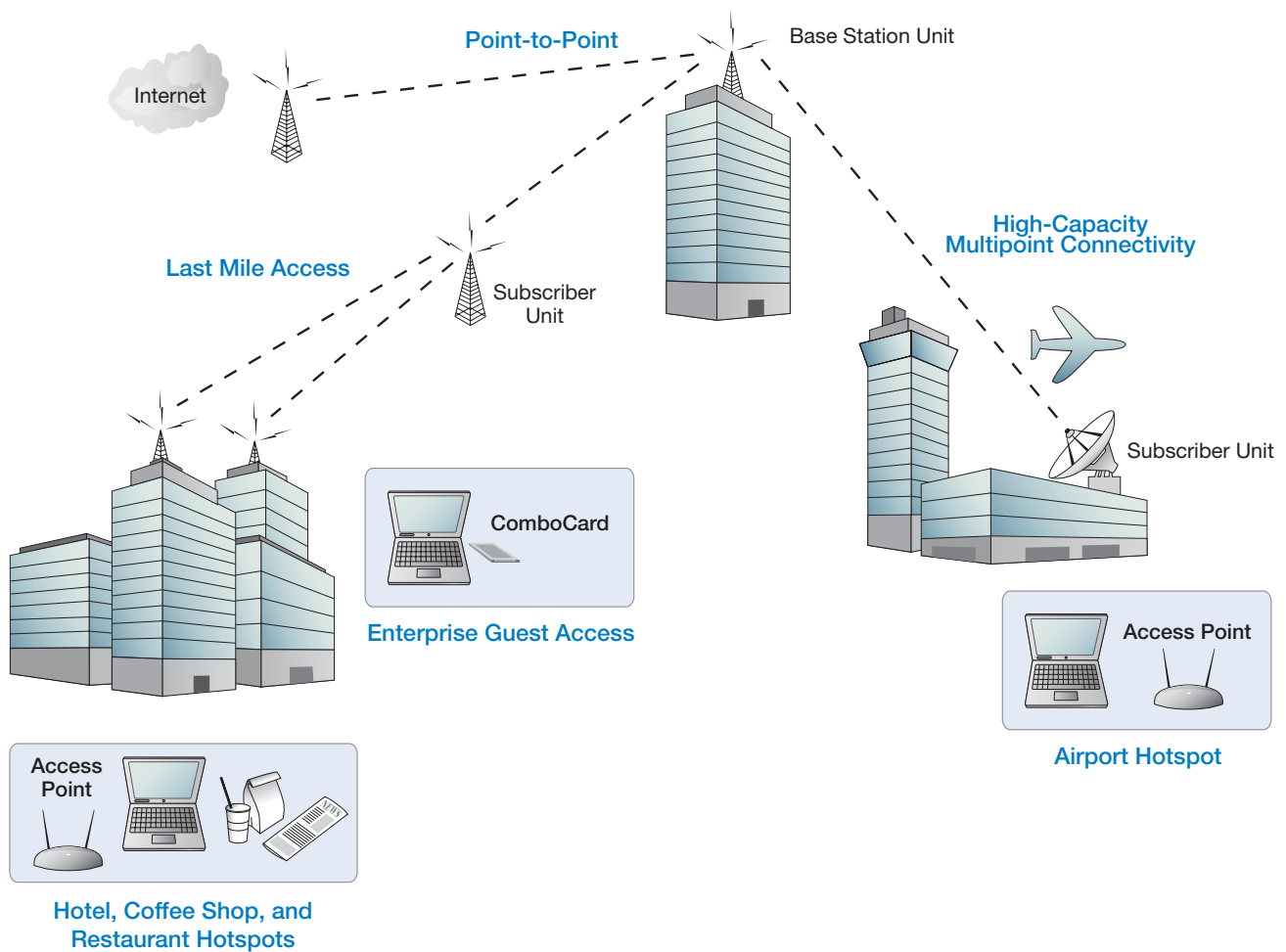
**Figure 1.** With the ratification of the 802.16a standard (Wi-MAX), comprehensive, secure and manageable wireless networks can now be deployed across metropolitan-sized areas using cost-effective, standards-based technologies.

The 802.11 standard is not static, but is continually under development to extend capabilities and provide simpler, faster, and more secure access. There is a strong emphasis on backward-compatibility, to enhance interoperability between existing devices and newer products based on more recently ratified standards. The most important current 802.11 standards include 802.11a (supports a maximum bandwidth of 54 Mbps in the 5 GHz band); 802.11b (supports up to 11 Mbps in the 2.4 GHz band); and 802.11g (establishes an additional modulation technique for the 2.4 GHz band, for bandwidths up to 54 Mbps).

These three standards offer flexible options for WLAN imple-mentations based on bandwidth, range and interoperability requirements. They are currently supported in Intel® Technology based single-band (802.11b) and dual-band (802.11a/b)

devices. In the first quarter of 2004, Intel will launch dual-band 802.11b/g devices, with tri-mode (802.11a/b/g) devices following in the second half of 2004. By deploying devices that support multiple standards, organizations will be able to upgrade existing wireless solutions, while maintaining inter-operability with older devices. In general, solution designers should take care to use only devices that have been certified by the Wi-Fi Alliance, to ensure a high level of cross-vendor interoperability.

- For more information about 802.11 standards, visit the Intel Web site at: http://www.intel.com/business/bss/ infrastructure/wireless/solutions/standards.htm

- For more information about Wi-Fi certified devices, visit the Wi-Fi Alliance Web site at: http://www.wi-fi.com

### IEEE 802.16a—Wireless Metropolitan Area Networks

The 802.16a standard was ratified by the IEEE in January 2003, extending the original 802.16 wireless standard, which was first passed in 1999. This standard established a broadly supported solution for comprehensive wireless networking across metropolitan-sized areas. 802.16a devices will support bandwidths up to 70 Mbps and ranges up to 30 miles (coverage under typical city conditions is approximately 3 to 5 miles per cell). The standard is designed to support robust security, frequency, channel and bandwidth control, and does not require uninterrupted line-of-site between devices—all of which are critical for providing cost-effective services in dense, urban environments. The standard also supports quality of service management, so audio, video and high-priority applications can share bandwidth and channels efficiently with lower priority transmissions. A single 802.16a base station can support hundreds or even thousands of mobile users and 802.11 WLAN hotspots.

Most importantly, devices based on the 802.16a standard will dramatically reduce the cost of deploying wireless networks in metropolitan areas, by providing efficient backhaul (connection to the Internet or other networks) for 802.11 access points. With this technology, there is no need to run network cables to the hundreds or thousands of 802.11 WLAN hotspots that might be deployed in a typical metropolitan network. It is only necessary to run cables to the much smaller number of 802.16a base stations, and these can be situated more flexibly to take advantage of existing cable installations, including high-bandwidth fiber backbones.

*WiMAX-Certified Products*

WiMAX (http://www.wimaxforum.org) is a nonprofit industry organization founded to support, promote and extend 802.16 and 802.16a based solutions, and to ensure a high-level of interoperability among compatible products from multiple vendors. WiMAX provides comprehensive test suites for product development and also certifies products for interoperability.

WiMAX is modeled after the highly successful Wi-Fi Alliance, which has fueled explosive growth for products based on the 802.11 standard. Both organizations allow vendors to focus on part of the solution, with confidence that their products will interoperate with other standards-based solutions. They also provide a high level of interoperability and investment protection for customers, since they can mix and match products from different vendors and scale solutions more reliably.

Intel is currently developing silicon-based building blocks for use in 802.16a compatible products. This will help to accelerate the development of reliable, high-performance WiMAX certified products and drive down customer costs.

### Mobile Devices Based on Intel Technology

Field use puts heavy demands on notebooks and other end-user devices. General ruggedness and reliability are important. Long battery life is especially critical to avoid downtime during a typical workday. However, long battery life must be balanced against performance requirements. As discussed in the next section, mobilized applications put a greater processing load on notebooks and other client devices. Strong security also draws substantial processing power for features such as encryption, real-time virus scanning and personal firewalls. Because of these demands, mobile workers need powerful systems rather than passive client devices that rely on centralized servers for processing power.

Field devices must also be portable, lightweight and easy to operate. Bulky systems, losable components (such as plug-in wireless cards), and slow or difficult log-on procedures can hamper productivity. Field workers may pack up, transport, and use their systems many times a day. In these circumstances, convenience is not just an amenity, but an important component of usability and productivity.

*Intel Centrino™ Mobile Technology for Laptops*

Intel Centrino mobile technology was designed from the ground up to address the needs of wireless workers. More than just a processor, this technology consists of optimized components that are designed to deliver an outstanding mobile experience. Intel Centrino mobile technology features integrated wireless LAN capability and breakthrough mobile performance, while enabling extended battery life in lighter, easier-to-carry notebook PCs. All of these components have been integrated and thoroughly tested for performance, compatibility and interoperability under a wide variety of conditions.[5]

- **Enhanced Field Productivity**—Intel Centrino mobile technology has become the foundation for a new generation of streamlined, lightweight notebook computers that are more portable, reliable and powerful. Breakthrough performance with unprecedented battery life enables field workers to stay more productive throughout the day.

- **Better Security Integration**—Intel Centrino mobile technology supports industry standard and leading third party security solutions enabling safer notebook connectivity. Some Intel Centrino mobile technology-based systems include Intel PROSet software with Profile Management that allows multiple profile set-up and automatic switching between profiles.[6]

- **Reduced TCO**—Intel Centrino mobile technology-based notebooks are supported by the Intel Stable Image Platform Program (Intel SIPP), which ensures the extended availability of configurations and components. Intel SIPP helps organizations maintain stable software images for longer periods, which can reduce qualification costs and provide a more stable and manageable environment. Intel Centrino mobile technology-based notebooks also support leading management standards, such as DMI (Desktop Management Interface) and WfM (Wired for Management), which provide a foundation for centralized, network-based management solutions. These features can be instrumental in reducing management costs for notebook computers, which typically account for 70-80% of the total cost of ownership.[7]

*Intel Personal Internet Client Architecture for Handheld Devices*

In addition to notebook computers, tablets and similar form factors, wireless handheld devices offer useful productivity advantages for many field workers. Personal digital assistants (PDAs), cell phones and other devices are increasing in power and functionality. Particularly noteworthy is the integration of cellular communications with application processing, which enables more functions to be supported using a single device.

To be effective in the field, these devices require many of the same features as notebooks, but in even smaller and more convenient packages. They must be reliable and easy to use, with a long battery life, substantial processing power, rich media capabilities, and a streamlined design.

The Intel Personal Internet Client Architecture (Intel PCA) is driving new levels of power, flexibility and innovation for these highly portable devices. As with Intel Centrino mobile technology, Intel PCA provides powerful and reliable silicon-based building blocks that enable easy and flexible expansion of wireless devices. Current advantages include high performance with exceptionally low power consumption, integration between cellular communications and application processing, and high-density memory solutions in ultra-small packages.

Intel PCA is based on Intel XScale® technology. Like Intel Centrino mobile technology, it will continue to incorporate the latest standards for wireless communications, management and security at the silicon level. As new standards emerge, the use of Intel technology-based devices will simplify integration into existing, standards-based application and networking environments, helping organizations to scale their solutions without major overhauls.

---

[5] Wireless connectivity and some features may require you to purchase or download additional software, services or external hardware. Availability of public wireless LAN access points is limited. System performance measured by MobileMark* 2002. System performance, battery life, wireless performance and functionality will vary depending on your specific hardware and software configurations. See www.intel.com/products/more_info for more information.

[6] PROSet and/or some security solutions may not be supported by your PC manufacturer. Check with your PC manufacturer for details on availability.

[7] *"…70 to 80 percent of the total cost of PC operation is unrelated to acquisition and deployment costs…;"* The Institute of Internal Auditors, *PC Management Best Practices: A Study of the Total Cost of Ownership, Risk, Security, and Audit,* Mark Salamasick & Charles Le Grand, 2003.

## Mobilized Applications

Depending on wireless coverage, most mobile field workers will regularly encounter interruptions to network connectivity. These interruptions need not disrupt productivity, as long as applications have been optimized for mobile use. In simplest terms, applications should allow mobile workers to perform all their key functions, even when a network connection is not available. Reconnection and data synchronization should then be automatic, seamless and secure when the wireless signal is once again available. When planning software enhancements, be aware that mobilized software is not for mobile users only, but is also beneficial in an office environment. Even users with traditional desktop PCs and wired LAN connections will experience enhanced productivity when the network is slow or unavailable.

The basic requirements for mobilized software include the following (Figure 2):

- **Offline Data Management**—Data should be asynchronously stored and managed all the way from the client to back-end applications and databases. In most cases, application functions and data should reside on the client device, so transactions and processing can be completed when a network connection is unavailable. As users roam between wireless access points, applications should automatically manage reconnection and re-authentication without user intervention. These basic capabilities should extend to management applications as well, so centralized support staff can efficiently deploy, upgrade and manage mobile systems.

- **Application Connectivity**—Applications should detect network state changes, and take the appropriate action to maintain the integrity, security and consistency of data and transactions.

- **Multiple Platform Support**—Mobilized software should be designed to support the growing diversity of computing devices (notebooks, PDAs, cell phones, etc.) by taking advantage of optimized software architectures and interoperable standards, such as Web services, XML, SOAP, and HTTP. Common development tools should be used across all platforms, to improve software consistency and reusability. Code can then be optimized to match specific device and connection attributes, such as bandwidth, power requirements, hardware architecture, display and storage limitations.

| Vector | Capability | Description |
|---|---|---|
| Offline Data Management | Synchronization | – Asynchronously store and manage data from client to back-end<br>– Include reliable messaging, transactions, and data coherency |
| | Security | – Application authentication while roaming<br>– Transparently re-authenticate on network re-connects<br>– Protect authentication credentials |
| | Manageability | – Managing the application environment to reduce IT TCO<br>– Simplify deployment, upgrade, and management models |
| Application Connectivity | Connectivity | – Detect network state changes and take the appropriate action |
| Multiple Platform Support | Cross Platform Support | – Develop a single core software architecture across all platforms<br>– Reuse technology standards and reuse code<br>– Use common development tools across platforms |
| | Characterization | – Identify key device and connection attributes like bandwidth, power scheme, hardware architecture, display and storage limitations. |
| Power and Performance | Power | – Reduce power consumption in order to extend battery life |
| | Performance | – Optimize application for performance |

Figure 2. Essential MSI Application Requirements: Baseline Needs
Mobilized software is essential to reap the full productivity benefits of wireless mobility. Key vectors for optimization include offline data management, application connectivity, multiple platform support and optimized power and performance.

- **Power and Performance**—Software code should be optimized for high performance and low power consumption. For example, applications should take advantage of Intel SpeedStep® technology, which offers multiple voltage and frequency operating points, enabling a better match of performance to application demand.

*The Advantages of Mobilized Software*

The advantages of mobilized software will be readily apparent in the field. Imagine a social worker visiting clients. Rather than drive across town to the office, he parks his car, logs onto the office network wirelessly, and checks his appointment schedule, which is automatically synchronized with his PDA and the centralized scheduling application for his department. Appropriate client files are automatically downloaded to his system. His first visit is in a thick-walled apartment building, where he is unable to connect to the network. However, all necessary data is now on his tablet computer. He updates records, takes notes and fills out any necessary forms during the visit. He might also write a quick e-mail requesting advice from his organization's psychiatric team.

Once outside where wireless access is available, his system automatically reconnects, sends his e-mail, submits his forms and updates his department's applications and databases based on his report. Before driving to his next appointment, he checks his schedule, e-mail and phone messages on his PDA. He sees an alert from his supervisor, asking if he can visit another client in the same neighborhood. He agrees. Once again, the necessary client files are downloaded to his notebook, and his schedule is automatically updated.

And so it goes throughout the day. Our social worker may take a few additional notes in his car using his PDA or notebook, but he never has to drive to and from the office, transcribe handwritten notes, or manually update his department's client database. He has stayed current with his e-mail and phone messages, documented his activities, and saved at least one return trip to the same neighborhood by accepting a new appointment request and by having all client information and forms available at each visit.

*Mobilizing Your Software*

Many application categories have already moved or are moving toward mobilized solutions. This is especially true for Customer Relationship Management (CRM) and other software solutions targeting sales force needs and other field functions. Application infrastructure solutions, such as IBM WebSphere*, BEA WebLogic* and Oracle Application Server*, have also been optimized to support mobile applications. These and similar products provide essential infrastructure services that can greatly simplify the process of optimizing specific applications for automatic synchronization, application connectivity and multiple platform support.

Intel has invested substantial resources toward industry-wide software mobilization. Intel software engineers provide detailed application architecture guidelines and are working with independent software vendors to help them optimize their applications for mobility. For more information, visit one of the following Web sites:

- http://www.intel.co.nz/business/bss/products/notebook/ mobileapps

- http://www.mobilizedsoftware.com

## Strong Security

Wireless applications, particularly in field settings, require careful attention to security. Safeguards should be geared to the nature of the network. For example, the wireless network may be private (e.g. for government use only) or public (a wireless infrastructure for business, private and government use). It could be free or subscription based. Network architects should take these issues into account in segmenting the network, and in establishing end-user authentication and authorization procedures.

Regardless of the network architecture, virtually anyone can monitor outdoor wireless transmissions using widely available and relatively inexpensive equipment. Strong encryption is therefore always essential if the privacy of transmitted information is to be protected. In addition, many of the most valuable uses of WLANs in the field involve providing access to back-end applications from wireless notebooks and PDAs. In these cases, it is important to assess security requirements for all applications, devices and wired networks that connect to the wireless infrastructure. The use of firewalls, authentication, anti-virus software, and Intrusion Detection Systems (IDS) should be considered for mobile clients, as well as for wired networks and associated applications. File encryption and strong end-user authentication (such as smart cards or biometric methods) may be appropriate for mobile devices, to prevent a lost or stolen device from compromising information security.

*Security Building Blocks for Wireless Networks.*

There is no one-size-fits all solution for WLAN security. The best choice depends on applications, implementation timelines, and the security framework for existing wired and wireless solutions. Depending on these issues, any of the following may be appropriate.

- **Original 802.11 Security Technologies**—Three security options are supported in all 802.11 devices: Service Set Identifiers (SSIDs), media access control (MAC) address filtering and Wired Equivalent Privacy (WEP). In general, these may be adequate for casual users, but not for security-sensitive applications. SSIDs are used to associate wireless devices with access points, and were never intended for security purposes. MAC address filtering offers good security, but the MAC addresses must be entered manually and can be spoofed by sophisticated hackers. WEP encrypts all transmissions, but uses static keys that can now be broken using downloadable tools from the Internet. It may be worthwhile to take advantage of these security options to provide additional layers of protection, but they should not be relied on if security is a significant issue.

- **Wi-Fi Protected Access (WPA)**—WPA has been certified by the Wi-Fi Alliance to provide a temporary solution to the weaknesses of WEP. It incorporates additional encryption and key protection measures and is now supported in all new Intel technology-based wireless devices. WPA provides a good security starting point for new implementations and is compatible with the upcoming 802.11i security standard (see below). It requires a firmware upgrade for WEP-enabled wireless access points.

- **Virtual Private Networking (VPN)**—VPN offers a proven security solution that is fully compatible with wireless implementations. It has been used successfully for many years to provide secure connections over the Internet using strong encryption and digital certificates. A particular advantage of VPN technology is that it is independent of the transmission medium. It provides application-based security that extends all the way from the client device to the VPN server, which is typically located behind the firewall of the wired LAN. Many organizations have existing VPN solutions that can be extended to the wireless network. For others, VPN will require an additional investment to design and implement.

- **802.11i Wireless Security Standard**—802.11i is a future standard that will simplify WLAN security solutions by building enterprise-class security support into all compatible access points and client devices, such as Intel Centrino mobile technology-based notebooks. It supports strong authentication, and improves encryption by using the Advanced Encryption Standard (AES). Depending on security requirements, it may eliminate the need for separate VPN solutions. However, it will require a hardware upgrade for most existing access points to handle the more demanding encryption algorithms of AES.

- **802.16a Security**—Privacy and encryption features are included in the 802.16a standard to support secure trans-missions and provide authentication and data encryption.

*Putting Security in Perspective*

Virtually any technology that improves access to information introduces new security issues. This has been true for net-worked PCs, mobile PCs, and the Internet, and it is now true for wireless mobility. Organizations that fail to leverage these new technologies put themselves at a competitive disadvan-tage. Organizations that implement them without architecting for security put their information and reputations at risk.

The answer is to carefully assess risks and benefits—based on the value and sensitivity of information—and invest in appropriate security safeguards. The standards and technologies listed above can be used to deploy strong, cost-effective security solutions, but they must be implemented as part of a comprehensive security program. Best practices—including user training, active monitoring and regular software updates—are as important as technology in establishing an effective security framework. For more information about wireless security, visit the Intel Web site, at http://www.intel.com/business/bss/products/client/pcrefresh/security.htm

## Wireless in Action

**The City of Westminster**

- **Better City Services at Reduced Cost**
- **£5M ROI Over 3 Years**
- **Growing Capacity for Mobility and Efficiency**

Located in the heart of London, the City of Westminster is the center of British government, and home to some of the most widely visited tourist attractions in the world. The Houses of Parliament are there, as well as Buckingham Palace, Trafalgar

Square and Westminster Cathedral. Hundreds of thousands of residents live within the city boundaries, and millions more work and visit there each year.

To improve key services and reduce operational costs, the city has established a 3-year plan to deploy a citywide wireless network for government functions, part of its broader City of Renewal and Customer Service initiatives. A phased approach will be used to test and rollout wireless services based on 802.11 (Wi-Fi) hotspots, 802.16 (WiMAX) backhaul stations and Intel Centrino mobile technology. The city expects to see a total ROI of more than £5M over the full 3 years.

*A Pilot Program that Pays for Itself*
To validate benefits and fine-tune solutions, the city has initiated a pilot program that includes the following parameters.

- **Wireless Users**—50

- **Wireless Network**—10 fixed wireless access points and 2 mobile wireless access points (mounted on vans), all with backhaul connections for linking with the Internet and back-office applications.

- **Security Monitors**—15 wireless cameras with microphones.

- **Applications**—A general mobile interface for all mobile users; and a new application to support major emergencies. The pilot program includes full testing for emergency teams, including a realistic simulation of an actual emergency.

The city has already had success deploying closed circuit television cameras for security monitoring, but the cost of installation has been high, primarily due to cabling costs. By deploying wireless cameras instead of wired models, and mounting them near existing power sources (e.g. lamp posts), the city will avoid approximately 84 percent of the installation costs, or about £29,550 per camera. These savings, alone, will more than cover the entire cost of the pilot program.

*A Phased Rollout with Positive ROI*
Over the following two to three years, the City of Westminster plans to equip 300 additional field professionals with Intel Centrino mobile technology-based notebooks and roll out about 4,000 additional wireless hotspots. Forecasts for the entire rollout show an estimated ROI of £5.5M (Table 1). Productivity benefits are estimated at approximately £2.6M/year. This is a conservative estimate based on a 25% productivity boost, or about 10 hours per week due to fewer trips to and from the office, real-time data entering, reduced errors, better scheduling of field work and reduced office costs through

| | 2004 | 2005 | 2006 | 2007 | 2008 |
|---|---|---|---|---|---|
| **Costs** | | | | | |
| Phase 1 | £5,982,575 | | | | £5,982,575 |
| Phase 2 | | £5,859,990 | | | £5,859,990 |
| Support and Maintenance | | | £1,189,013 | £1,189,013 | £2,378,025 |
| Total Costs | £5,982,575 | £5,859,990 | £1,189,013 | £1,189,013 | £14,220,590 |
| **Cash Inflow** | | | | | |
| Productivity: Road Warriors | £1,312,500 | £2,625,000 | £2,625,000 | £2,625,000 | £9,187,500 |
| Others | £421,125 | £1,403,750 | £1,403,750 | £1,403,750 | £4,632,375 |
| Accommodation | £450,000 | £900,000 | £900,000 | £900,000 | £3,150,00 |
| Capital Saved: CCTV | £4,846,200 | | | | £4,846,200 |
| Total Cash Inflow | £7,029,825 | £4,928,750 | £4,928,750 | £4,928,750 | £21,816,075 |
| **Net Cashflow** | £1,047,250 | -£931,240 | £3,739,738 | £3,739,738 | £7,595,486 |
| **Discounted Rate** | 100% | 87% | 76% | 66% | |
| **Discounted Cashflow** | £1,047,250 | -£809,744 | £2,827,779 | £2,458,938 | £5,524,193 |
| **Forecasted 3 YR NPV   £5,524,193** | | | | | |

**Table 1.    ROI Calculation—Wireless City Project**
Return on Investment calculations for the City of Westminster's phased rollout of wireless capabilities.

space sharing. With ongoing process improvements, the city expects to see productivity gains of 30-42%, based on 12 to 17 hours savings per worker per week.

During this same period, plans call for an additional 164 wireless security cameras. This is expected to accelerate the existing camera deployment program, while saving an additional £4.8M through reduced installation costs. The city will also deploy wireless bridges for many of its building-to-building network connections. Though this will incur £174K in installation and setup costs, the city expects to save £192K/year by terminating existing contracts to service providers for leasing network bandwidth.

*Expansion Opportunities*

With a growing wireless infrastructure in place, it will be increasingly cost-effective to extend wireless capabilities to additional workers and functions, and to upgrade mobile capabilities for existing services. Opportunities for expansion include deployment to more than 500 additional workers, event monitoring and civic watch (through wireless cameras and microphones), noise and traffic monitoring for capacity and service planning, increased mobility for parking attendants, and an expansion of the existing network of information kiosks to improve on-site services and information for residents and tourists. The city may also consider working with local service providers to lease wireless bandwidth to businesses and private citizens.

With the rapid advances underway in wireless and mobile technologies, one thing is certain. City of Westminster officials can rest assured that new capabilities and applications will continue to expand the value of their wireless infrastructure.[7]

## Rio Rancho, New Mexico

- **Wireless Mobility for Everyone**
- **A Public Infrastructure from Private Providers**
- **A Business and Lifestyle Differentiator for "The City with Vision"**

Rio Rancho, New Mexico has different needs then the City of Westminster, and a very different plan for rolling out wireless capabilities. Rio Rancho wants a public wireless infrastructure that will empower existing residents and businesses, and help attract newcomers to the city. City planners envision ubiquitous wireless connectivity that will enable mobile users to go virtually anywhere within city limits—including inside homes and businesses—and connect instantly to the Internet and to business networks.

Instead of only the airport and a few cafés, wireless services will be available at public parks, restaurants, medical waiting rooms and city streets. People will be able to run errands, take the kids to soccer, go out to lunch—and stay connected. The service will be available to everyone, and its ubiquity will ensure seamless roaming with no need for multiple accounts, multiple passwords or multiple usage fees. It will also eliminate the need for private wireless access devices in most locations. All anyone will need is an appropriately configured notebook or other wireless device. Of course, there may be some locations where wireless services may not penetrate, such as basements and thick-walled buildings. If desired, these locations could be serviced with private wireless access points that could then be linked to the public network.

To bring this vision to fruition, the city of Rio Rancho is working with private vendors to establish a ubiquitous, high-bandwidth wireless infrastructure. A Telcom will provide the fiber backbone, and the city is looking at individual wireless service providers to determine an appropriate technology strategy and equipment choices. The entire network will be privately owned, run and managed, and available to all on a subscription or pay-per-use basis.

This wireless network will substantially enhance the value of wireless for every organization and individual in Rio Rancho. It will provide a foundation for enhanced services and better cross-organizational collaboration for government agencies, with similar benefits for private businesses. Users can take advantage of VPN technologies to protect sensitive data and communications over the wireless network, just as many already do for secure transactions over the Internet. Once this network is in place, Rio Rancho will be one of the best places in the world to take advantage of wireless mobility.

---

[7] The Wireless City: A Report on Mobile and Broadband Wireless Computing for the City of Westminister.

# Recommendations for Success

Whether built by private providers or public funds, a wireless city is a major undertaking, and yet the potential benefits are simply too great to ignore. The key is to avoid basing investments and designs on an abstract vision of universal mobility. A better approach is to plan a phased implementation that delivers measurable value at each step—while building toward a ubiquitous and scalable infrastructure. The following recommendations can help.

1. **Plan and Implement a Focused Pilot Program.** Look for wireless solutions to current challenges. For example:

   - **Public Safety and Security Monitoring at Trouble Spots.** Wireless greatly reduces the cost of installing surveillance cameras.

   - **Strategically Placed Access Points for Field Staff.** A dozen or so scattered access points could allow inspectors, police and other field workers to synchronize with back-end applications, send e-mail and access the Internet, by driving a short distance, rather than returning to the office.

   - **Team Coordination for Major Emergencies or Events.** Vehicles with wireless backhaul capabilities could allow teams to communicate wirelessly onsite at nearly any location, greatly improving information flow and interdepartmental coordination.

   - **Building-to-Building Bridging.** Broadband wireless connections between buildings can eliminate the high cost of leased line connections.

2. **Focus on Applications.** Value is achieved only when processes and information flow are improved for specific workers and functions. Current applications and work processes should be evaluated to understand the potential impact of wireless communications. It is important to understand the full scope of project requirements, because success will often require software changes and end-user training, in addition to providing wireless access points and devices.

3. **Plan for Growth.** Short-term success depends on well-planned projects with verifiable ROI. Long-term success depends on leveraging scalable technologies and standards-based solutions in each project, so the value of the wireless infrastructure continues to grow.

   - **Understand the Technology Roadmap for Wireless Technologies** based on key standards, such as 802.11, 802.16 and 802.20 (WWAN) technologies. Also keep an eye on cellular standards and technologies—such as General Packet Radio Service (GPRS) and Global System for Mobile Communication (GSM)—for wireless wide area network solutions. These technologies may be important for extending service to outlying areas and interconnecting with national or regional wireless resources.

   - **Rely on Fully-Ratified Standards and Certified Products.** Notebooks based on Intel Centrino mobile technology and handheld devices based on Intel PCA offer a good starting point. Though deploying non-standard solutions may make sense in small networks, the risk is substantial for any large, metropolitan sized implementation.

   - **Develop Internal Standards for All Aspects of Your Wireless Solution**, including software development and integration, access point configuration, security solutions, and end-user devices. These standards should extend across all projects and organizational boundaries, to achieve the best possible value from the wireless infrastructure.

   - **Revisit Your Wireless Plans Frequently.** Technologies, products and business models are evolving rapidly.

4. **Leverage Your Growing Infrastructure.** As your network and expertise grows, costs for new implementations will be lower. Continue to look for value-driven applications that leverage the existing network, and also justify infrastructure expansion.

5. **Plan for a Manageable Environment.** By their nature, wireless access points and end-user devices are widely distributed. You can greatly reduce your total cost of ownership by planning for efficient and secure management of these devices over the wireless network. For best results, management for notebooks and other wireless devices should be integrated with your larger PC fleet management strategies.[8]

---

[8] For more information, see the Intel white paper, *PC Lifecycle Management—Tools and Strategies for Reducing TCO and Optimizing Total Value*. Available at http://www.intel.com/business/bss/products/client/management.pdf

**6. Consider Revenue Generation Opportunities.** A wireless infrastructure is an increasingly valuable asset. Consider teaming with service providers to leverage your network and to satisfy business and/or consumer demand.

**7. Continue to Mobilize Your Applications.**

- Look for mobile optimization from all your software vendors and/or in-house development teams.

- Focus on standards-based software technologies (XML, SOAP, HTTP, etc.) to improve scalability and interoperability.

# Conclusion

In time, every city will be wireless. The benefits in productivity and convenience are simply too compelling to ignore. Workers become more efficient, organizations collaborate more effectively, residents can access information from almost anywhere, and improved services can be delivered at reduced cost. Based on these advantages, forward-thinking cities are beginning to explore their options now. The most successful implementations will focus on:

- Identifying opportunities for which wireless mobility can deliver immediate value.

- Beginning with manageable pilot programs to validate benefits and refine solutions prior to wide-scale deployment.

- Taking a cost-effective, phased approach to building the wireless infrastructure.

- Using standards-based technologies and certified products to provide a scalable solution that can grow as needs and technologies evolve, with particular emphasis on Wi-Fi (802.11) and WiMAX (802.16a) certified products.

As wireless solutions evolve, Intel will continue to work with the wireless industry to advance and promote standards that improve performance, interoperability and security.

Intel will also implement the latest standards in reliable, high-performance silicon for cost-effective support in Intel Centrino mobile technology-based notebooks and Intel PCA-based handheld devices. As wireless networks are deployed throughout the world, governments, businesses and individuals can count on these devices to deliver increasing power and functionality for staying connected and productive wherever they happen to be.

For more information, see the following Intel White Papers:

- Extending Enterprise Solutions for Mobility

- Deploying Secure Wireless Networks: Intel's strategies to minimize WLAN risk

- IEEE 802.16* and WiMAX: Broadband access for everyone

Or visit the following Web sites:

- http://www.intel.com/business/bss/infrastructure/wireless/index.htm

- http://www.intel.com/business/bss/products/client/pcrefresh/unwire.htm

- http://www.mobilizedsoftware.com/

[1] XXXXXXX